Gen Docket No. 0951

Gregory Intoccia

To: Gregory Intoccia
Subject: FW: Workshop

Attachments: 2009-10-30-google-fcc-cybersecurity-response.pdf

2009-10-30-google-fcc-cybersec...

```
-----Original Message-----
From: Marc Donner [mailto:donner@google.com]
Sent: Thursday, October 29, 2009 10:31 PM
To: Joy Ragsdale
Cc: Jennifer Manner
Subject: Re: FCC Cyber Security Workshop Follow-up

Attached is a PDF of our detailed responses to the questions you sent us on October 9th.
Would you like us to send a paper copy with a wet ink signature as well?

Best regards,

Marc Donner
=====
On Fri, Oct 9, 2009 at 18:01, Joy Ragsdale <Joy.Ragsdale@fcc.gov> wrote:
> Mr. Donner,
>
>
>
> In order to ensure we have a more complete record, we would appreciate
> your comments in response to the attached questions by November 1, 2009.
>
>
>
>
>
> Thank you
>
>
>
> Joy M. Ragsdale, Attorney
>
> FCC, Public Safety & Homeland Security
>
> Policy Division
>
> w) 202-418-1697
>
>
>
> *** Non-Public: For Internal Use Only ***
>
>
>
>
>
>
>
>
>
```

--
=====
Marc Donner
Google
76 Ninth Avenue
New York, NY 10011
+1-212-565-1977

Google

76 Ninth Avenue, 4th Floor Tel: 212.565.0000
New York, NY 10011 Fax: 212.565.0001

2009 October 30

Jennifer A. Manner
Deputy Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
Jennifer.Manner@fcc.gov

Dear Ms. Manner,

Thank you for the opportunity to participate in the FCC's October 2, 2009 Cyber Security Workshop. Below are the follow up questions that you sent out on October 9 with our thoughts.

- What would motivate more network providers to adopt approaches to improve security when effectiveness depends on what other providers do, as might be the case with authentication, routing security, and DNS security? Are there policies that the U.S. government should consider in the broadband plan to encourage this?
    - Require ISPs to implement BCP 38 and 84 (ingress filtering). The specific document (http://www.ietf.org/rfc/rfc3704.txt) has details. The key objective is for networks to discard packets that have obviously falsified source address.
    - (One of our experts thinks that most ISPs already do. Compliance numbers should be examined before rules are implemented.)
- With respect to information sharing about outcomes and results, what incentives are needed to encourage service providers to report more data about the occurrence and resolution of cyber security incidents to their customers, the FCC, other government or security-focused agencies, and competitive service providers?
    - The incentive of also receiving information from the FCC or other government agencies should be enough to motivate sharing, but this incentive turns on establishing a track record of actually engaging in two-way information flow with the private sector (consistent with national and homeland security, of course).
    - The FCC should establish a network statistics bureau and couple each requirement for submission of data with an appropriate publication of statistical summaries of the data gathered.
- Should there be a uniform or baseline definition of "cyber security incident" that mandates when service providers report to their customers, the FCC, other government or security-focused agencies, and competitive service providers a security incident that may be global affecting?
    - It's probably premature for a standard definition. We should be able to identify some of the common modes now, like for instance DDOS SYN floods. The FCC could sponsor a data base (US CERT?) of attacks and diagnoses. The FCC could establish a contact registry for ISPs to use when unwelcome traffic is flowing into their network from another operator.
- Currently, there are many private and public sector agencies that offer and encourage the adoption of security best practices. How can the FCC or other government-supported entities serve as a repository for centralizing these different best practices?
    - The FCC should channel its efforts in this area through NIST.

- What could ISPs do to offer their subscribers more security to protect end users intellectual property and data integrity and compromise from cyber thieves that may gain access to this information using keyloggers, IP masking or other virtual means to access the end users data?
  - Encouraging service providers (not ISPs, but entities like banks and other such providers) to adopt better authentication than userid/password.
- Would it be possible to implement hashing, 256 or 512 Bit encryption, SHA 64+1, RSA Token Authentication to ensure the protection of the end users data?
  - If the endpoint is compromised by keylogger or other credential stealing techniques, stronger encryption of stored data or network links doesn't fix anything. One-time passwords or other token-based authentication don't prevent man-in-the-middle attacks (MITM), but they do provide some mitigation against keyloggers. Beyond strengthening the credentials, protecting the logged on session merits attention.
- How have more complicated supply chains from diverse sources, including from outside the United States, introduced vulnerabilities into information and/or network technologies and affected cyber security? Are commercial service providers adequately addressing such vulnerabilities and, if not, what can be done to better address these concerns?
  - The Internet is inherently international in nature. The place of origin of "components" (software, accessories, end-user hardware, communications gear) does not implicitly vet their trustworthiness. While in some very specific application domains, such as battlefield communications equipment, one might worry that foreign-built components may have been exposed to tampering that was targeting just such equipment, in general this is not a tractable approach.
  - Open source and strong interface and protocol specifications are the most powerful and effective techniques to ameliorate the concerns outlined in this question with respect to software.
- What metrics, resources or tools can be used to measure whether an organization can sustain its security practices in times of crisis?
  - The presence of aggressive test and exercise programs within the organization. The ability of the test organization to conduct tests without prior notice and without appeal by the tested organization. Response time and recovery time in the face of lesser and prior crises. Detailed post-mortem documentation of incidents.
- What are some ways that government can incent industry to promote the increased use of integrity check and authentication systems?
  - Disclosure of security breaches. Put appropriate clauses in government contracts. Most vendors will find it easier to put integrity checks in all products rather than just those aimed at the government.
- The panelists expressed concern that infrastructure security problems often result from end users not using secure applications to protect their home computers. What additional steps or educational tools are needed to make people aware of the need to secure their computers?
  - Public awareness campaign plus clear unambiguous guidance on what to do.

Very truly yours,

Marc Donner

Federal Communications Commission
Washington, D.C. 20554

October 9, 2009

Marc Donner
Engineering Director
Google Health, Google Finance, AdWords Engineering
76 Ninth Avenue, 4th Floor
New York, NY 10011

Re: National Broadband Plan Proceeding, Docket No. 09-51

Dear Mr. Donner:

Thank you, very much for your participation in the FCC's October 2, 2009 Cyber Security Workshop. The Workshop was very enlightening and provided important information that will be considered in developing a National Broadband Plan.

As a follow-up to the workshop and in order to ensure we have a complete record, we would appreciate it if you could provide your comments in response to the following questions by November 1, 2009. Of course, your answers will be made part of the public record for the Broadband Plan proceeding.

<u>Questions</u>

- What would motivate more network providers to adopt approaches to improve security when effectiveness depends on what other providers do, as might be the case with authentication, routing security, and DNS security? Are there policies that the U.S. government should consider in the broadband plan to encourage this?
- With respect to information sharing about outcomes and results, what incentives are needed to encourage service providers to report more data about the occurrence and resolution of cyber security incidents to their customers, the FCC, other government or security-focused agencies, and competitive service providers?
- Should there be a uniform or baseline definition of a "cyber security incident" that mandates when service providers report to their customers, the FCC, other government or security-focused agencies, and competitive service providers a security incident that may be global affecting?
- Currently, there are many private and public sector agencies that offer and encourage the adoption of security best practices. How can the FCC or other government-supported entities serve as a repository for centralizing these different best practices?
- What could ISPs do to offer their subscribers more security to protect end users intellectual property and data integrity and compromise from cyber thieves that may

gain access to this information using keyloggers, IP masking or other virtual means to access the end users data?

- Would it be possible to implement hashing, 256 or 512 Bit encryption, sha 64+1, RSA Token Authentication to ensure the protection of the end users data?
- How have more complicated supply chains from diverse sources, including from outside the United States, introduced vulnerabilities into information and/or network technologies and affected cyber security? Are commercial service providers adequately addressing any such vulnerabilities and, if not, what can be done to better address these concerns?
- What metrics, resources or tools can be used to measure whether an organization can sustain its security practices in times of crisis?
- What are some ways that government can incent industry to promote the increased use of integrity check and authentication systems?
- The panelists expressed concern that infrastructure security problems often result from end users not using security applications to protect their home computers. What additional steps or educational tools are needed to make people aware of the need to secure their computers?

Thank you once again. Your contribution will help us shape a bold and innovative vision for how we can develop initiatives to strengthen our nation's broadband networks and protect them from potentially damaging and global affecting cyber attacks. If you have any questions or comments please feel free to contact me at (202) 418-3619 at your convenience.

Sincerely,

Jennifer A. Manner
Deputy Chief
Public Safety and Homeland Security Bureau
Jennifer.Manner@fcc.gov